

NFC UICC Test Book
Version 1.0
01 May 2015

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2015 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction 4
1.1 Overview 4
1.2 Scope 4
1.3 Definition of Terms 4
1.4 Abbreviations 5
1.5 Document Cross-References 7
1.6 Conventions 8
2 Test Environment 9
2.1 Applicability 9
2.1.1 Format of the Table of Features 9
2.1.2 Format of the Applicability Table 9
2.1.3 Status and Notations 10
2.1.4 Table of Optional Features 10
2.1.5 Applicability Table 12
2.2 General Consideration 13
2.2.1 Test Cases Definition 13
2.2.2 Pass Criterion 13
2.2.3 Future Study 14
2.3 Test Equipment 14
3 Certifications 14
3.1 GlobalPlatform Card Compliance 14
3.1.1 Format of the Table of Test Suite Options 14
3.1.2 UICC Compliance Test Suite 15
3.1.3 UICC Contactless Extension Test Suite 20
3.1.4 UICC Memory Management Extension Test Suite 22
3.1.5 SWP and HCI Test Suite 23
3.1.6 Secure Element Access Control Test Suite 25
3.1.7 UICC SCP81 Extension Test Suite 27
3.1.8 Common Implementation Configuration Test Suite 29
3.2 Common Criteria 30
3.2.1 (U)SIM Java Card Platform Protection Profile 30
4 Test Specifications 31
4.1 Format of the Table of Test Specification Options 31
4.2 ETSI TS 102 268 31
4.3 ETSI TS 103 115 31
4.4 ETSI TS 102 431 32
4.5 ETSI TS 102 226 Testing 33
5 Other Tests Cases 33
5.1 Cryptographic Algorithms 33
5.1.1 General Overview 33
5.1.2 Conformance Requirements 33
5.1.3 Constants Definition 33

5.1.4 Referenced APDUs 34
5.1.5 Test Cases 35
5.2 ACTIVATE Proactive Command 48
5.2.1 General Overview 48
5.2.2 Conformance Requirements 48
5.2.3 Test Cases 48
5.3 CASD Management Data 48
5.3.1 General Overview 48
5.3.2 Conformance Requirements 48
5.3.3 Test Cases 49
Annex A SP Applications 50
A.1 Basic Application 50
A.2 Sensitive Application 50
Annex B Java Card 51
Annex C Document Management 52
C.1 Document History 52
C.2 Document Owner 52

1 Introduction

1.1 Overview

The main aim of the GSMA NFC activities is to accelerate the commercial launch of UICC-based NFC services in a number of markets by ensuring interoperability of services.

The NFC Test Book stream is part of GSMA's NFC activities. The GSMA SGP.03 NFC UICC Requirements Specification document [1] defines a common framework of requirements for UICCs to support UICC-based NFC services. Some requirements are already certified by other industry bodies and some others refer to test specifications developed by other organisations.

The participating GSMA SIM NFC members have identified the related certifications and test specifications which describe tests cases to be used for checking UICC compliance with GSMA NFC UICC requirements. In addition, relevant test cases have been developed for requirements not covered by existing certification or test specifications. All this information is collated in the present document.

Therefore, this Test Book contains:

- Certification references
- Test specifications
- Test cases

The Test Book is developed in such a way that the test case descriptions are generic, but provide repeatable instructions so that any Test Lab can implement these test cases without further clarification.

The Test Lab will be responsible for the test case implementations (which are tool specific) as set out in the Test Book.

The GSMA will retain the ownership to any rights of all the test cases and other intellectual property set out in the Test Book.

1.2 Scope

This document is intended for:

- Test Labs that execute the testing
- Manufacturers
- Operators

1.3 Definition of Terms

Term	Description
Application	Instance of an Executable Module after it has been installed and made selectable.
Application Group	An Application Group is a concept that allows group member Applications to be represented to the end-user by a dedicated group Head Application.

Term	Description
Basic Logical Channel	The permanently available interface between the UICC and an external entity. The Basic Logical Channel is numbered zero.
Device	NFC equipment into which an UICC and a communication module are inserted (e.g. Mobile Device).
Executable Load File	An on-card container of one or more Application's executable code as defined in GlobalPlatform Card Specification [13].
Executable Module	The on-card executable code of a single Application present within an Executable Load File as defined in GlobalPlatform Card Specification [13].
Head Application	The Head Application is a Contactless Application that owns the Display Control Information and the Contactless Protocol Parameters of an Application Group.
Issuer Security Domain	An SD on the UICC as defined by GlobalPlatform Card Specification [13].
Manufacturer	UICC manufacturer.
Member Application	An Application part of an Application Group.
Operator	Refers to an MNO who provides the technical capability to access the mobile environment using an OTA communication channel. The Operator is the UICC Issuer. An Operator provides an UICC OTA Management System, which is also called the OTA Platform.
OTA Platform	An MNO platform for remote management of UICCs.
Supplementary Logical Channel	Up to 19 additional interfaces (other than the permanently available Basic Logical Channel) between the UICC and an external entity. Each Supplementary Logical Channel is numbered from 1 up to 19.
Test Book	Current document describing the test cases that allow testing of the requirements listed in the GSMA NFC UICC Requirements Specification [1].
Test Lab	This refers to a Test Lab which will implement the test cases according to the Test Book for testing NFC UICCs. The Test Lab would also need to declare that they are compliant with the criteria of the GSMA Test Lab self-accreditation process.
Token	A cryptographic value provided by an UICC Issuer as proof that a Delegated Management operation has been authorized.
UICC Issuer	Entity that owns the UICC and is ultimately responsible for the behaviour of the UICC.

1.4 Abbreviations

Acronyms	Description
AC	Access Control
AID	Application Identifier
AES	Advanced Encryption Standard
AM	Authorized Management
APDU	Application Protocol Data Unit
API	Application Programming Interface

Acronyms	Description
ARA-C	Access Rule Application Clients
ARA-M	Access Rule Application Master
ARF	Access Rules File
ATR	Answer To Reset
ATS	Answer To Select
BIP	Bearer Independent Protocol
CASD	Controlling Authority Security Domain
CAT_TP	Card Application Toolkit Transport Protocol
CBC	Cipher Block Chaining
CC	Cryptographic Checksum
CCRA	Common Criteria Recognition Arrangement
CLA	Class byte of the command message
CLT	Contactless Tunnelling
DAP	Data Authentication Pattern
DEK	Data Encryption Key
DES	Data Encryption Standard
DM	Delegated Management
DS	Device Simulator
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
ELF	Executable Load File
EM	Executable Module
EMVCo	Europay Mastercard Visa & Co
ETSI	European Telecommunications Standards Institute
FFS	For Future Study
GSMA	GSM Association
HCI	Host Controller Interface
HCP	Host Controller Protocol
HID	Host Identifier
HTTP	HyperText Transfer Protocol
IEC	International Electrotechnical Commission
INS	Instruction byte of the command message
ISD	Issuer Security Domain
ISO	International Organization for Standardization
KCV	Key Check Value
KENC	Encryption Key
KIC	Key and algorithm Identifier for ciphering
KID	Key and algorithm Identifier for RC/CC/DS

Acronyms	Description
KMAC	Message Authentication Code Key
KVN	Key Version Number
LC	Exact length of data in a case 3 or case 4 command
LE	Maximum length of data expected in response to a command
MAC	Message Authentication Code
MNO	Mobile Network Operator
NFC	Near Field Communication
OTA	Over The Air
P1	Reference control parameter 1
P2	Reference control parameter 2
PKI	Public Key Infrastructure
RAM	Remote Application Management
R-APDU	Response APDU
REQ	Requirement
RSA	Rivest / Shamir / Adleman asymmetric algorithm
SCP	Secure Channel Protocol
SD	Security Domain
SE	Secure Element
SEAC	Secure Element Access Control
SIM	Subscriber Identity Module
SMS	Short Message Service
SMS-PP	SMS - Point to Point
SP	Service Provider
SPI	Security Parameters Indication
SREJ	Selective Reject
SW	Status Word
SWP	Single Wire Protocol
TAR	Toolkit Application Reference
TLS	Transport Layer Security
TS	Technical Specification
UICC	Universal Integrated Circuit Card (USIM)
USB	Universal Serial Bus
UUT	UICC Under Test

1.5 Document Cross-References

Ref	Title
[1]	GSMA NFC UICC Requirements Specification - Version 5.0
[2]	GSMA NFC SP Applet Development Guideline - Version 3.0

[3]	GlobalPlatform Card - Composition Model - Version 1.1
[4]	ETSI TS 102 268 Smart Cards; Test specification for UICC Application Programming Interface (API) for Java Card™ - Version 6.1.0 (2013-06)
[5]	ETSI TS 103 115 Smart Cards; Test specification for UICC Application Programming Interface for Java Card™ for Contactless Applications; Test Environment and Annexes - Version 9.3.0 (2013-12)
[6]	ETSI TS 102 613 Smart Cards; UICC – Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics - Version 9.3.0 (2012-09) or later
[7]	ETSI TS 102 622 Smart Cards; UICC – Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) - Version 9.4.0 (2011-09) or later
[8]	ETSI TS 102 241 Smart Cards; UICC Application Programming Interface (UICC API) for Java Card™ - Version 9.2.0 (2012-03) or later
[9]	ETSI TS 102 705 Smart Cards; UICC Application Programming Interface for Java Card™ for Contactless Applications - Version 9.2.0
[10]	ETSI TS 102 431 Smart Cards; Test specification for the Transport Protocol of CAT Applications (CAT_TP) validation - Version 7.1.0 (2008-03)
[11]	ETSI TS 102 127 Smart Cards; Transport protocol for CAT applications - Version 6.13.0 (2009-04) or later
[12]	GlobalPlatform Card Technology - Secure Channel Protocol 03 - Card Specification v2.2 - Amendment D - Version 1.1
[13]	GlobalPlatform Card Specification - Version 2.2.1
[14]	RFC 2246 - The TLS Protocol - Version 1.0
[15]	RFC 4346 - The TLS Protocol - Version 1.1
[16]	RFC 5246 - The TLS Protocol - Version 1.2
[17]	ETSI TS 102 226 Smart Cards; Remote APDU structure for UICC based applications - Version 9.6.0 (2013-01) or later
[18]	ETSI TS 102 225 Smart Cards; Secured packet structure for UICC based applications - Version 9.2.0 (2012-03) or later
[19]	GlobalPlatform Card - UICC Configuration - Version 1.0.1
[20]	GlobalPlatform Card - Contactless Services - Card Specification v2.2 - Amendment C - Version 1.1
[21]	GlobalPlatform Card - Mapping Guidelines of Existing GlobalPlatform v2.1.1 Implementation on v2.2.1 - Version 1.0.1
[22]	ETSI TS 102 223 Smart Cards; Card Application Toolkit (CAT) - Version 9.4.0 (2012-03) or later

1.6 Conventions

Throughout this document, normative requirements are highlighted by use of capitalized key words as described below.

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY" in this document are to be interpreted as follows:

SHALL - This word, or the terms "REQUIRED", mean that the definition is a mandatory requirement of the specification.

SHALL NOT - This phrase means that the definition is a mandatory prohibition of the specification.

SHOULD - This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT - This phrase means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY - This word means that an item is truly optional. One supplier may choose to include the item because a particular marketplace requires it or because the supplier feels that it enhances the product while another supplier may omit the same item.

2 Test Environment

2.1 Applicability

2.1.1 Format of the Table of Features

The columns in Table 4 have the following meaning:

Column	Meaning
Feature	The optional feature supported or not by the implementation.
Mnemonic	The mnemonic column contains mnemonic identifiers for each item.
Support	The support columns are to be filled in by the Manufacturer. The following common notations are used for the support column in Table 4: Y or y: supported by the implementation. N or n: not supported by the implementation.

Table 1: Format of the Table of Features

2.1.2 Format of the Applicability Table

The applicability of every certification, test specification or test case in Table 5 is formally expressed by the use of Boolean expression defined in the following clause.

The columns in Table 5 have the following meaning:

Column	Meaning
Section	The "Section" column gives the section number in the present document where the corresponding item in the "Name" column is described.
Name	In the "Name" column, the name of the concerned item is found. It could be a certification, a test specification or a test case.
Applicability	The "Applicability" column indicates the applicability status of the corresponding item (see Table 3 for the applicability status notation).

Table 2: Format of the Applicability Table

2.1.3 Status and Notations

The following notations are used for the “Applicability” column:

Applicability Code	Meaning
M	Mandatory - the capability is required to be supported.
O	Optional - the capability may be supported or not.
N/A	Not Applicable - in the given context, it is impossible to use the capability.
Ci	Conditional - the requirement on the capability depends on the support of other items. "i" is an integer identifying an unique conditional status expression which is defined immediately following the table. For nested conditional expressions, the syntax "IF ... THEN (IF ... THEN ... ELSE...) ELSE ..." is to be used to avoid ambiguities.

Table 3: Status and Notations

2.1.4 Table of Optional Features

The Manufacturer shall state the support of optional features in Table 4. See clause 2.1.1 for the format of Table 4. Items indicated as O_XYZ refer to features supported by the UICC.

Item	Feature	Mnemonic	Support
	Transport Options		
1	CAT_TP mechanism see Note 1	O_CATTP	
2	RAM over HTTP see Note 1	O_RHTTP	
3	SEAC management using SMS	O_AC_SMS	
	CAT_TP Options		
4	Window size > 1	O_WIN_S	
5	Simultaneous open requests	O_SOPEN	
6	Segmentation of outgoing data	O_SEG	
7	Local port definition in active open request	O_LPORT	
8	Passive mode	O_PASS_M	
	Applicative Options		
9	MIFARE for Mobile	O_MIFARE	
10	ARA-M	O_ARA_M	
	UICC Configuration Options		
11	API org.globalplatform.SecureChannelx	O_API_SCX	
12	API org.globalplatform.SecureChannel.encryptData	O_API_ENC	
13	Card Reset management	O_RST	
14	Tag ‘CF’ in `INSTALL` parameters	O_CF	
15	Tag ‘2F00’ on `GET DATA`	O_2F00	
16	Tag ‘FF1F’ on `GET DATA`	O_FF1F	
17	Tag ‘FF20’ on `GET DATA`	O_FF20	

Item	Feature	Mnemonic	Support
18	Tag 'FF21' on GET DATA	O_FF21	
19	SET STATUS of SD and its associated Applications	O_STATUS	
20	PUT KEY one by one for a SCP key	O_PUT_K	
21	DELETE key command for a SD with AM	O_DEL_K	
22	DELETE key command without key identifier provided	O_DEL_KID	
23	DELETE key command by providing key version number and key identifier	O_DEL_KVN	
24	At least two Supplementary Logical Channels	O_2LC	
25	At least three Supplementary Logical Channels	O_3LC	
26	DAP computation using DES	O_DAP_DES	
27	DAP computation using RSA	O_DAP_RSA	
28	DES for Token computation	O_TOK_DES	
29	RSA for Token computation	O_TOK_RSA	
30	RSA algorithm with 1024 bytes key length	O_RSA	
31	RSA key update	O_RSA_UPD	
32	Keyset loading restrictions as defined in GlobalPlatform Mapping Guidelines [21]	O_KEY_LOAD	
33	Confidential setup of initial secure channel keys	O_CSISC	
34	Confidential setup of SCP keys: Scenario #1 (PKI)	O_SC1_PKI	
35	Confidential setup of SCP keys: Scenario #2.A	O_SC2A	
36	Token length coded on 1 byte when size equal to 128 bytes	O_TOKLEN_1	
37	Token length coded on 2 bytes when size equal to 128 bytes	O_TOKLEN_2	
	SCP03 Options		
38	BEGIN R-MAC and END R-MAC SESSION commands	O_RMAC	
39	ISD has the Card Reset privilege	O_ISD_RST	
40	ISD has the Final Application privilege	O_ISD_FINAL	
	UICC Contactless Options		
41	Application Group: Head Application required to be created before Member Applications	O_AG_HEAD	
42	Cumulative delete	O_CD	
43	Cumulative granted memory	O_CGM	
44	Memory quota 'C8' in INSTALL parameters	O_MEM_Q	
45	Reserved memory 'D8' in INSTALL parameters	O_MEM_R	
	SCP81 Options		
46	SCP81: TLS 1.0	O_TLS_10	
47	SCP81: TLS 1.1	O_TLS_11	
48	SCP81: TLS 1.2	O_TLS_12	
49	AES DEK key on SCP81	O_AES_DEK	
	SWP Options		

Item	Feature	Mnemonic	Support
50	Class A on ETSI TS 102 221 interface	O_CLASS_A	
51	CLT, ISO/IEC 18092	O_CLT_F	
52	SREJ	O_SREJ	
53	Sliding window size of 4	O_WS_4	
54	USB as per ETSI TS 102 600	O_102_600	
55	Extended bit durations down to 0,590 µs	O_EXT_TL	
56	Extended bit durations up to 10 µs	O_EXT_TU	
57	UICC sends upper layer indication that the UICC requires no more activity on this interface	O_UPPL	
	HCI Options		
58	WHITELIST, as specified in ETSI TS 102 622, contains the HID of at least one further host	O_WL_NE	
59	Card emulation Type B'	O_CE_TBP	
60	Card emulation Type F	O_CE_TF	
61	HCP message size greater than supported buffer size	O_HCP	
	UICC API Contactless Options		
62	Reader mode Type A	O_RM_TA	
63	Reader mode Type B	O_RM_TB	
Note 1: The UUT shall support at least one of O_CATTP and O_RHTTP options			

Table 4: UICC Optional Features

2.1.5 Applicability Table

Table 5 specifies the applicability of each certification, test specification or test case defined in this Test Book to the UUT. See clause 2.1.2 for the format of Table 5.

Applicability conditions are defined in Table 6.

Section	Name	Applicability
	Certifications	
3.1.2	GlobalPlatform – UICC Compliance Test Suite	M
3.1.3	GlobalPlatform – UICC Contactless Extension Test Suite	M
3.1.4	GlobalPlatform – UICC Memory Management extension Test Suite	C5
3.1.5	GlobalPlatform – SWP and HCI Test Suite	M
3.1.6	GlobalPlatform – Secure Element Access Control Test Suite	C1
3.1.7	GlobalPlatform – UICC SCP81 extension Test Suite	C2
3.1.8	GlobalPlatform – Common Implementation Configuration Test Suite / Common_SCP03 Package	C4
3.2.1	EAL4+ Common Criteria – (U)SIM Java Card Platform Protection Profile PU-2009-RT-79-2.0.2	O
	Test Specifications	

Section	Name	Applicability
4.2	ETSI TS 102 268	M
4.3	ETSI TS 103 115	M
4.4	ETSI TS 102 431	C3
4.5	ETSI TS 102 226 Testing	M
Test Cases		
0	TC.AES.16.SCP80: SCP80 using AES with 16 bytes key length	M
5.1.5.2	TC.AES.32.SCP80: SCP80 using AES with 32 bytes key length	M
5.1.5.3	TC.3DES.24.SCP80: SCP80 using Triple DES with 24 bytes key length	M
5.2.3	ACTIVATE Proactive Command Testing	M
5.3.3	CASD Management Data Testing	C6

Table 5: Applicability of Tests

Conditional Item	Condition
C1	IF (O_ARA_M) THEN M ELSE N/A
C2	IF (O_RHTTP OR (NOT O_CATTP)) THEN M ELSE N/A
C3	IF (O_CATTP OR (NOT O_RHTTP)) THEN M ELSE N/A
C4	IF (O_MIFARE) THEN M ELSE N/A
C5	IF (O_CD OR O_CGM) THEN M ELSE N/A
C6	IF (O_CSISC) THEN M ELSE N/A

Table 6: Conditional Items Referenced by Table 5

2.2 General Consideration

This section contains some general considerations about the test cases defined in this Test Book. Note that some test suites and test specifications are referred to in sections 3 and 4. Consequently, the following sub sections shall only apply if not differently specified in these related documents.

2.2.1 Test Cases Definition

Test descriptions are independent.

For each test described in this document, a chapter provides a general description of the initial conditions valid for the whole test. This description is completed by specific configurations to each individual sub-case.

After completing the test, the configuration is reset before the execution of the following test.

2.2.2 Pass Criterion

A test execution is considered as successful only if the test procedure was fully carried out successfully.

A test execution is considered as failed if the tested feature provides an unexpected behaviour. Note that, in the test sequences defined in section 5 of this Test Book, a test execution shall

also be considered as failed when an error occurs during the steps indicated with a white background in the tables.

A test execution is considered as inconclusive when the pass criteria cannot be evaluated due to issues during the setup of the initial conditions. Note that, in the test sequences defined in section 5 of this Test Book, a test execution shall also be considered as inconclusive when an error occurs during the steps indicated in the tables with a pink background.

2.2.3 Future Study

Some of the test cases described in this Test Book are FFS (For Future Study). This means that some clarifications are expected at the requirement level to conclude on a test method.

Test Labs will indicate these tests as “Not Tested” in the test report.

2.3 Test Equipment

This chapter aims at describing test equipment to be used to run required test cases.

For certification and test specification test cases, Test Labs shall follow the related test equipment requirements.

For test cases defined in this Test Book, the test equipment shall provide a Device Simulator which is connected to the UUT during test procedure execution. Test Labs shall meet the following requirements:

- be able to send and receive APDU commands to the UICC
- be able to provide results of the tests

3 Certifications

This section lists the UICC certifications that the UICC shall undergo to comply with GSMA requirements. These certifications are delivered by certification bodies providing a Letter of Approval/Compliance.

These certifications are mainly intended to guarantee the correct functioning of specific use cases, specifically mobile payments.

The Operator expects to receive from the Manufacturer the Letter of Approval for the listed certifications at the same time as the test report corresponding to the test cases in this Test Book.

3.1 GlobalPlatform Card Compliance

Certifications listed in this section are provided by the GlobalPlatform Card Compliance Program.

3.1.1 Format of the Table of Test Suite Options

To execute a test suite, the Manufacturer shall state specific options listed in a `CardOptions.xml` file. For each test suite described in the following sections, a table, containing the expected options values, is specified.

The columns of this table have the following meaning:

Column	Meaning
Test Suite Option	The “Test Suite Option” column contains the name and the description of the option defined by GlobalPlatform Card Compliance. Note that, for readability reason, the prefix “conf_” has been deleted from all option names.
Support	The support columns are to be filled in by the Manufacturer. The following common notations are used for the support column: Y or y: expected to be supported by the implementation. N or n: expected to not be supported by the implementation. O_XYZ: refers to the support of the related feature described in Table 4.

Table 7: Format of the Table of Test Suite Options

3.1.2 UICC Compliance Test Suite

The UUT shall take the “UICC Compliance Test Suite Version 2.3.0” certification test cases.

Note that if any revisions are performed on this test suite, the version 2.3.0.X, with X the number of the last revision, shall apply.

3.1.2.1 Technical Specifications

This certification relates to technical specifications listed in Table 8.

Technical Specifications
GlobalPlatform Card - UICC Configuration - Version 1.0.1
GlobalPlatform Card Specification - Version 2.2.1
GlobalPlatform Card - Mapping Guidelines of Existing GlobalPlatform v2.1.1 Implementation on v2.2.1 - Version 1.0.1
GlobalPlatform Card - Confidential Card Content Management - Card Specification v2.2 - Amendment A - Version 1.0.1
ETSI TS 102 127 Smart Cards; Transport protocol for CAT applications (Release 6)
ETSI TS 102 221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 7)
ETSI TS 102 225 Smart Cards; Secured packet structure for UICC based applications (Release 7)
ETSI TS 102 226 Smart Cards; Remote APDU structure for UICC based applications (Release 7 + CR SCPt080562)
ETSI TS 102 223 Smart Cards; Card Application Toolkit (CAT) (Release 7)
ETSI TS 101 220 Smart Cards; ETSI numbering system for telecommunication application providers (Release 7+ CR SCPt080563 and SCPt080564)

Table 8: UICC Compliance Test Suite - Technical Specifications

3.1.2.2 Required Options Values

It shall be verified that in the `CardOptions.xml` file provided by the Manufacturer the "expected to be supported" options are set to true and the "expected not to be supported" options are set to false. See clause 3.1.1 for the format of Table 9.

Test Suite Option	Support
algo_RSA1024_Supported	O_RSA

Test Suite Option	Support
Indicates that RSA algorithm, with 1024 bytes key length, is supported by the UICC or not.	
AmendmentCSupported *Defines if the "GlobalPlatform Card Amendment C [20]" is supported by the UICC or not. This is only relevant to determine if a life cycle state shall be encoded with 1 or 2 bytes.*	Y
ApduDeleteKeySupportForSdWithAuthorizedManagement *Defines if the `DELETE` key command is supported for a SD with AM.*	O_DEL_K
ApduDeleteKeySupportKeyVersionNumber *Defines if the `DELETE` key command is supported without key identifier provided.*	O_DEL_KID
ApduDeleteKeySupportKeyVersionNumberAndKeyId *Defines if the `DELETE` key command is supported by providing key version number and key identifier.*	O_DEL_KVN
ApduDeleteSupportForSdWithDelegatedManagement *Defines if the `DELETE` command is supported for a SD with DM.*	Y
ApduGetDataSupport_2F00 *Indicates if the `GET DATA` command supports the tag '2F00' on SD.*	O_2F00
ApduGetDataSupport_FF1F *Indicates if the `GET DATA` command supports the tag 'FF1F' on SD.*	O_FF1F
ApduGetDataSupport_FF20 *Indicates if the `GET DATA` command supports the tag 'FF20' on SD.*	O_FF20
ApduGetDataSupport_FF21 *Indicates if the `GET DATA` command supports the tag 'FF21' on SD.*	O_FF21
ApduGetStatusSupportForOtherSd *Defines if the `GET STATUS` command is supported for any SD (without AM nor DM).*	Y
ApduGetStatusSupportForSdWithDelegatedManagement *Defines if the `GET STATUS` command is supported for a SD with DM.*	Y
ApduInitializeUpdateSupportForOtherSD *Defines if the `INITIALIZE UPDATE` command is supported for any SD (without AM nor DM).*	Y
ApduInstallParametersSupportedTagCF *Defines if the tag 'CF' in `INSTALL` command data field is supported.*	O_CF
ApduInstForExtraditionForSdWithAuthorizedManagement	Y

Test Suite Option	Support
Defines if the `INSTALL FOR EXTRADITION` command is supported for a SD with AM (also applies to the ISD).	
ApduInstForExtraditionForSdWithDelegatedManagement *Defines if the `INSTALL FOR EXTRADITION` command is supported for a SD with DM.*	Y
ApduInstForInstallAndInstForMakeSelectableSupportForSdWithAuthorizedManagement *Defines if the `INSTALL FOR INSTALL AND MAKE SELECTABLE` command is supported for a SD with AM (also applies to the ISD).*	Y
ApduInstForInstallAndInstForMakeSelectableSupportForSdWithDelegatedManagement *Defines if the `INSTALL FOR INSTALL AND MAKE SELECTABLE` command is supported for a SD with DM.*	Y
ApduInstForLoadAndApduLoadSupportForSdWithAuthorizedManagement *Defines if the `INSTALL FOR LOAD` and `LOAD` commands are supported for a SD with AM (also applies to the ISD).*	Y
ApduInstForLoadAndApduLoadSupportForSdWithDelegatedManagement *Defines if the `INSTALL FOR LOAD` and `LOAD` commands are supported for a SD with DM.*	Y
ApduInstForPersoSupportForSdWithAuthorizedManagement *Defines if the `INSTALL FOR PERSONALIZATION` command is supported for a SD with AM (also applies to the ISD).*	Y
ApduInstForPersoSupportForSdWithDelegatedManagement *Defines if the `INSTALL FOR PERSONALIZATION` command is supported for a SD with DM.*	Y
ApduInstForRegUpdateSupportForSdWithAuthorizedManagement *Defines if the `INSTALL FOR REGISTRY UPDATE` command is supported for a SD with AM (also applies to the ISD).*	Y
ApduPutKeyCreationSCPSingleKeySupported *Indicates that, on the `PUT KEY` command, the following feature is supported: put the key identifier one by one for a SCP key.*	O_PUT_K
ApduPutKeySupportForOtherSd *Defines if the `PUT KEY` command is supported for any SD (without AM nor DM).*	Y
ApduPutKeySupportForSdWithDelegatedManagement *Defines if the `PUT KEY` command is supported for a SD with DM.*	Y
ApduSetStatusSDAndAssociatedSupported	O_STATUS

Test Suite Option	Support
Indicates if the `SET STATUS` command supports the parameter P1 equal to "Security Domain and its associated Applications" (60h).	
ApduSetStatusSupportForOtherSd *Defines if the `SET STATUS` command is supported for any SD (without AM nor DM).*	Y
ApduStoreDataSupportForOtherSd *Defines if the `STORE DATA` command is supported for any SD (without AM nor DM).*	Y
atLeastOneSupplementaryLc *Indicates that at least one Supplementary Logical Channel is supported.*	Y
atLeastThreeSupplementaryLc *Indicates that at least three Supplementary Logical Channels are supported.*	O_3LC
atLeastTwoSupplementaryLc *Indicates that at least two Supplementary Logical Channels are supported.*	O_2LC
DapComputationUsingDesSupported *Indicates that, DAP computation using DES, is supported by the UICC or not.* see Note 1	O_DAP_DES
DapComputationUsingRsaSupported *Indicates that, DAP computation using RSA, is supported by the UICC or not.* see Note 1	O_DAP_RSA
FeatureCardResetManagement *Indicates if the Card Reset feature is managed by the UICC or not.*	O_RST
GPAPI_EncryptDataSupported *Defines if the API `org.globalplatform.SecureChannel.encryptData` is supported by the UICC or not (if not supported, it might be for security reasons).*	O_API_ENC
implementationExtraditeSecurityDomainSupported Defines *if `INSTALL FOR EXTRADITION` is supported to extradite a SD.*	Y
implementationSupportForDelegatedManagement *Defines if DM is supported by the UICC or not.*	Y
implementationSupportGlobalLockPrivilege *Defines if Global Lock privilege is supported by the UICC or not.*	Y
implementationSupportGlobalRegistryPrivilege *Defines if Global Registry privilege is supported by the UICC or not.*	Y
implementationSupportGPAPISecureChannelX	O_API_SCX

Test Suite Option	Support
Defines if the API `org.globalplatform.SecureChannelx` is supported by the UICC or not.	
implementationSupportsInstallTagEA *Declares if the tag 'EA' in the `INSTALL` parameters is supported by the UICC or not.*	Y
implementationSupportsSCP03 *Defines if SCP03 is supported by the UICC or not.*	O_MIFARE
implementationSupportsSCP80OverBIPCATTP *Configuration flag used in the processing of SCP80 scripts. It declares that the UICC supports BIP CAT_TP as the data bearer for SCP80 testing.*	O_CATTP
implementationSupportsSCP80OverSMS *Configuration flag used in the processing of SCP80 scripts. It declares that the UICC supports SMS as the data bearer for SCP80 testing.*	Y
implementationSupportsTLVEncodedSDInstallParam *Defines if SD `INSTALL` parameters shall be provided as TLV encoded.*	Y
implementationSupportsTrustedPath *Defines if Trusted Path privilege is supported by the UICC or not.*	Y
implementationSupportSupplementarySD *Defines if SSD is supported by the UICC or not.*	Y
implementationUsesDESForTokenComputation *Indicates that the implementation supports DES for token computation.* see Note 2	O_TOK_DES
implementationUsesRSAForTokenComputation *Indicates that the implementation supports RSA for token computation.* see Note 2	O_TOK_RSA
ISD_Configured_With_SCP03 *Defines if the ISD is configured with an SCP03 keyset.*	O_MIFARE
KeyRsaUpdate_NotSupported *Indicates that a SD will not accept the update of an existing RSA key.*	O_RSA_UPD
KeySetLoadUsageRestriction - *Indicates if the SSD does not support loading RSA key with the secure channel services of its associated SD* - *Indicates if the SSD does not support the initialization of a key identifier set to zero or greater than 3* - *Indicates if the SSD does not support the update of an RSA key*	O_KEY_LOAD

Test Suite Option	Support
- *Indicates if the SSD does not support the creation of an RSA key for anything else than DAP* - *Indicates if the SSD does not support the creation of an RSA key when the modulus length is not 128 bytes or when the exponent length is not 1 or 3*	
Length_Token_128_coded_as_one_byte *Indicates that, the Token length is coded on one byte as '80' when the length is equal to 128 bytes.* see Note 3	O_TOKLEN_1
Length_Token_128_coded_as_two_bytes *Indicates that, the Token length is coded on two bytes as '81 80' when the length is equal to 128 bytes.* see Note 3	O_TOKLEN_2
onlyBasicLc *Indicates that only the Basic Logical Channel is supported and no other one.*	N
SCENARIO1_NON_PKI_SUPPORTED *Indicates that, for Confidential Card Content Management, SCENARIO1 (NON PKI) is supported by the UICC or not.*	N
SCENARIO1_PKI_SUPPORTED *Indicates that, for Confidential Card Content Management, SCENARIO1 (PKI) is supported by the UICC or not.*	O_SC1_PKI
SCENARIO2A_SUPPORTED *Indicates that, for Confidential Card Content Management, SCENARIO2A is supported by the UICC or not.*	O_SC2A
SCENARIO2B_SUPPORTED *Indicates that, for Confidential Card Content Management, SCENARIO2B is supported by the UICC or not.*	O_CSISC
SupportDataRetrievalForElfAndEm *Indicates if the `GET STATUS` command allows retrieving information for ELF and EM.*	Y
Note 1: The UUT shall support at least one of O_DAP_DES and O_DAP_RSA options *Note 2: The UUT shall support either O_TOK_DES or O_TOK_RSA options* *Note 3: The UUT shall support at least one of O_TOKLEN_1 and O_TOKLEN_2 options*	

Table 9: UICC Compliance Test Suite - Options

3.1.3 UICC Contactless Extension Test Suite

The UUT shall take the “UICC Contactless Extension Test Suite Version 3.3.0” certification test cases.

Note that if any revisions are performed on this test suite, the version 3.3.0.X, with X the number of the last revision, shall apply.

3.1.3.1 Technical Specifications

This certification relates to technical specifications listed in Table 10.

Technical Specifications
GlobalPlatform Card - UICC Configuration - Contactless Extension - Version 1.0
GlobalPlatform Card Specification - Version 2.2.1
GlobalPlatform Card - Contactless Services - Card Specification v2.2 - Amendment C - Version 1.0.1
GlobalPlatform Card - UICC Configuration - Version 1.0.1
ISO/IEC 14443-3 Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anti-collision
Application Programming Interface, Java Card™ Platform, v3.0.1, Classic Edition

Table 10: UICC Contactless Extension Test Suite - Technical Specifications

3.1.3.2 Required Options Values

It shall be verified that in the `CardOptions.xml` file provided by the Manufacturer the "expected to be supported" options are set to true and the "expected not to be supported" options are set to false. See clause 3.1.1 for the format of Table 11.

Test Suite Option	Support
Card_require_Application_Group_Created *Indicates that the UICC requires that Application Group is well created (Head created before the Members).*	O_AG_HEAD
implementationSupportsForwardedCASDData *Indicates that the implementation supports the "Forwarded CASD Data" specification introduced in "GlobalPlatform Card Amendment C [20]".*	Y
SCENARIO1_NON_PKI_SUPPORTED *Indicates that, for Confidential Card Content Management, SCENARIO1 (NON PKI) is supported by the UICC or not.*	N
SCENARIO1_PKI_SUPPORTED *Indicates that, for Confidential Card Content Management, SCENARIO1 (PKI) is supported by the UICC or not.*	O_SC1_PKI
SCENARIO2A_SUPPORTED *Indicates that, for Confidential Card Content Management, SCENARIO2A is supported by the UICC or not.*	O_SC2A
SCENARIO2B_SUPPORTED *Indicates that, for Confidential Card Content Management, SCENARIO2B is supported by the UICC or not.*	O_CSISC

Table 11: UICC Contactless Extension Test Suite - Options

3.1.4 UICC Memory Management Extension Test Suite

The UUT may take the “UICC Memory Management extension Test Suite Version 1.0.0” certification test cases (depending of the O_CGM and O_CD support).

Note that if any revisions are performed on this test suite, the version 1.0.0.X, with X the number of the last revision, shall apply.

3.1.4.1 Technical Specifications

This certification relates to technical specifications listed in Table 12.

Technical Specifications
GlobalPlatform Card - UICC Configuration - Contactless Extension - Version 1.0
GlobalPlatform Card Specification - Version 2.2.1
GlobalPlatform Card - Contactless Services - Card Specification v2.2 - Amendment C - Version 1.0.1
GlobalPlatform Card - UICC Configuration - Version 1.0.1
ISO/IEC 14443-3 Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anti-collision
Application Programming Interface, Java Card™ Platform, v3.0.1, Classic Edition

Table 12: UICC Memory Management Extension Test Suite - Technical Specifications

3.1.4.2 Required Options Values

It shall be verified that in the `CardOptions.xml` file provided by the Manufacturer the "expected to be supported" options are set to true and the "expected not to be supported" options are set to false. See clause 3.1.1 for the format of Table 13.

Test Suite Option	Support
Card_require_Application_Group_Created *Indicates that the UICC requires that Application Group is well created (Head created before the Members).*	O_AG_HEAD
implementationSupportsCumulativeDelete *Indicates that the UICC supports cumulative delete.*	O_CD
implementationSupportsCumulativeGrantedMemory *Indicates that the UICC supports cumulative granted memory.*	O_CGM
Install_Parameter_Support_Memory_Quota_C8 *Indicates that the UICC supports the memory quota ‘C8’ in `INSTALL` parameters.* see Note 1	O_MEM_Q
Install_Parameter_Support_Reserved_Memory_D8 *Indicates that the UICC supports the reserved memory ‘D8’ in `INSTALL` parameters.* see Note 1	O_MEM_R

Test Suite Option	Support
Note 1: The O_MEM_Q and O_MEM_R options may be only supported if O_CGM is supported	

Table 13: UICC Memory Management Extension Test Suite - Options

3.1.5 SWP and HCI Test Suite

The UUT shall take the “SWP and HCI Test Suite Version 2.0.3” certification test cases.

Note that if any revisions are performed on this test suite, the version 2.0.3.X, with X the number of the last revision, shall apply.

3.1.5.1 Test Specifications

This certification is based on test specifications listed in Table 14.

Test Specifications
ETSI TS 102 694-2 Smart Cards; Test specification for the Single Wire Protocol (SWP) interface; Part 2: UICC features - Version 10.1.0
ETSI TS 102 695-2 Smart Cards; Test specification for the Host Controller Interface (HCI); Part 2: UICC features - Version 9.3.0

Table 14: SWP and HCI Test Suite - Test Specifications

3.1.5.2 Technical Specifications

This certification relates to technical specifications listed in Table 15.

Technical Specifications
ETSI TS 102 221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics - Version 9.1.0 or later
ETSI TS 102 613 Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics see Note 1
ETSI TS 102 622 Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) see Note 2
Note 1: For the purpose of this document, the version of the technical specification implemented on the UICC shall be the [6]. *Note 2: For the purpose of this document, the version of the technical specification implemented on the UICC shall be the [7].*

Table 15: SWP and HCI Test Suite - Technical Specifications

3.1.5.3 Required Options Values

It shall be verified that in the `CardOptions.xml` file provided by the Manufacturer the "expected to be supported" options are set to true and the "expected not to be supported" options are set to false. See clause 3.1.1 for the format of Table 16.

Test Suite Option	Support
SWP Options	
SWP_O_102_600	O_102_600

Test Suite Option	Support
Defines if USB as per ETSI TS 102 600 is supported by the UICC or not.	
SWP_O_102_622 *Defines if the HCI as per ETSI TS 102 622 is supported by the UICC or not.*	Y
SWP_O_CLASS_A *Defines if the class A on ETSI TS 102 221 interface is supported by the UICC or not.*	O_CLASS_A
SWP_O_CLT_A *Defines if the CLT, ISO/IEC 14443 Type A is supported by the UICC or not.*	Y
SWP_O_CLT_F *Defines if the CLT, ISO/IEC 18092 is supported by the UICC or not.*	O_CLT_F
SWP_O_EXTENDED_T_LOWER *Defines if the extended SWP bit durations down to 0,590 µs is supported by the UICC or not.*	O_EXT_TL
SWP_O_EXTENDED_T_UPPER *Defines if the extended SWP bit durations up to 10 µs is supported by the UICC or not.*	O_EXT_TU
SWP_O_SREJ *Defines if SREJ is supported by the UICC or not.*	O_SREJ
SWP_O_TERM_CAP *Defines if `TERMINAL CAPABILITY` is supported by the UICC or not.*	Y
SWP_O_UPPL_NO_MORE_ACT *Indicates that the UICC sends upper layer indication that the UICC requires no more activity on this interface.*	O_UPPL
SWP_O_WS_3 *Defines if the sliding window size of 3 is supported by the UICC or not.*	Y
SWP_O_WS_4 *Defines if the sliding window size of 4 is supported by the UICC or not.*	O_WS_4
HCI Options	
HCI_O_102_613 *Indicates if the data link layer, specified in ETSI TS 102 613, is being used.*	Y
HCI_O_CLT_A *Defines if the CLT, ISO/IEC 14443 Type A is supported by the UICC or not.*	Y
HCI_O_LINK_MAN *Defines if the link management gate is supported by the UICC or not.*	Y

Test Suite Option	Support
HCI_O_TYPE_A *Defines if the card emulation Type A is supported by the UICC or not.*	Y
HCI_O_TYPE_B *Defines if the card emulation Type B is supported by the UICC or not.*	Y
HCI_O_TYPE_B_PRIME *Defines if the card emulation Type B' is supported by the UICC or not.*	O_CE_TBP
HCI_O_TYPE_F *Defines if the card emulation Type F is supported by the UICC or not.*	O_CE_TF
HCI_O_WHITELIST_NON_EMPTY *Indicates if the WHITELIST, specified in ETSI TS 102 622, contains the HID of at least one further host.*	O_WL_NE

Table 16: SWP and HCI Test Suite - Options

3.1.6 Secure Element Access Control Test Suite

The UUT may take the "Secure Element Access Control Test Suite Version 1.0.8" certification test cases (depending of the O_ARA_M support).

Note that if any revisions are performed on this test suite, the version 1.0.8.X, with X the number of the last revision, shall apply.

In addition, the requirements related to ARA-C and ARF are out of the scope defined in this test suite. Consequently, testing these features remains under the responsibility of each MNO or SP.

3.1.6.1 Technical Specifications

This certification relates to technical specifications listed in Table 17.

Technical Specifications
GlobalPlatform Device Technology - Secure Element Access Control - Version 1.0
GlobalPlatform Card Specification - Version 2.2.1
GlobalPlatform Card - Confidential Card Content Management - Card Specification v2.2 - Amendment A - Version 1.0.1
GlobalPlatform Card - Contactless Services - Card Specification v2.2 - Amendment C - Version 1.0.1
GlobalPlatform Card - Remote Application Management over HTTP - Card Specification v2.2 - Amendment B - Version 1.1.1
ETSI TS 102 127 Smart Cards; Transport protocol for CAT applications (Release 6)
ETSI TS 102 221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 6)
ETSI TS 102 225 Smart Cards; Secured packet structure for UICC based applications (Release 6)
ETSI TS 102 226 Smart Cards; Remote APDU structure for UICC based applications (Release 6)
ETSI TS 102 241 Smart Cards; UICC Application Programming Interface (UICC API) for Java Card™ (Release 6)

Technical Specifications
ETSI TS 102 622 Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) (Release 7)
GSMA NFC Handset APIs & Requirements - Version 2.0

Table 17: Secure Element Access Control Test Suite - Technical Specifications

3.1.6.2 Required Options Values

It shall be verified that in the `CardOptions.xml` file provided by the Manufacturer the "expected to be supported" options are set to true and the "expected not to be supported" options are set to false. See clause 3.1.1 for the format of Table 18.

Test Suite Option	Support
implementationSupportsSCP80OverBIPCATTP *Defines if the RAM (related to SEAC) over CAT_TP is supported by the UICC or not.*	O_CATTP
implementationSupportsSCP80OverSMS *Defines if the RAM (related to SEAC) over SMS is supported by the UICC or not.*	O_AC_SMS
implementationSupportsSCP81_TLS1_0 *Defines if TLS 1.0, as defined in RFC 2246 [14], is supported by the UICC or not.* see Note 1	O_TLS_10
implementationSupportsSCP81_TLS1_1 *Defines if TLS 1.1, as defined in RFC 4346 [15], is supported by the UICC or not.* see Note 1	O_TLS_11
implementationSupportsSCP81_TLS1_2 *Defines if TLS 1.2, as defined in RFC 5246 [16], is supported by the UICC or not.* see Note 1	O_TLS_12
ISD_Configured_With_SCP02 *Defines if the ISD is configured with an SCP02 keyset.*	Y
ISD_Configured_With_SCP03 *Defines if the ISD is configured with an SCP03 keyset.*	O_MIFARE
RemoteApplicationManagement_Based_on_SCP02 *Defines if the RAM (related to SEAC) over SCP02 is supported by the UICC or not.*	Y
RemoteApplicationManagement_Based_on_SCP03 *Defines if the RAM (related to SEAC) over SCP03 is supported by the UICC or not.*	O_MIFARE
RemoteApplicationManagement_Based_on_SCP80 *Defines if the RAM (related to SEAC) over SCP80 is supported by the UICC or not.*	Y
RemoteApplicationManagement_Based_on_SCP81	O_RHTTP

Test Suite Option	Support
Defines if the RAM (related to SEAC) over SCP81 is supported by the UICC or not.	
Note: The UUT shall be certified SEAC through all Secure Channel and transport protocols supported by the implementation. One `CardOptions.xml` per protocol shall be provided to the Test Lab. *Note 1: If the UUT supports O_RHTTP, at least one of O_TLS_10, O_TLS_11 and O_TLS_12 options shall be supported.*	

Table 18: Secure Element Access Control Test Suite - Options

3.1.7 UICC SCP81 Extension Test Suite

The UUT may take the “UICC SCP81 extension Test Suite Version 1.8.0” certification test cases (depending of the O_RHTTP support).

Note that if any revisions are performed on this test suite, the version 1.8.0.X, with X the number of the last revision, shall apply.

3.1.7.1 Technical Specifications

This certification relates to technical specifications listed in Table 19.

Technical Specifications
GlobalPlatform Card - Remote Application Management over HTTP - Card Specification v2.2 - Amendment B - Version 1.1.1
GlobalPlatform Card Specification - Version 2.2
ETSI TS 102 223 Smart Cards; Card Application Toolkit (CAT) (Release 10)
ETSI TS 102 226 Smart Cards; Remote APDU structure for UICC based applications (Release 10)

Table 19: UICC SCP81 Extension Test Suite - Technical Specifications

3.1.7.2 Required Options Values

It shall be verified that in the `CardOptions.xml` file provided by the Manufacturer the "expected to be supported" options are set to true and the "expected not to be supported" options are set to false. See clause 3.1.1 for the format of Table 20.

Test Suite Option	Support
algo_AES_Supported *This option is deprecated.*	O_AES_DEK
AmendmentCSupported *Defines if the “GlobalPlatform Card Amendment C [20]” is supported by the UICC or not. This is only relevant to determine if a life cycle state shall be encoded with 1 or 2 bytes.*	Y
ApduGetStatusSupportForOtherSd *Defines if the `GET STATUS` command is supported for any SD (without AM nor DM).*	Y
ApduInitializeUpdateSupportForOtherSD	Y

Test Suite Option	Support
Defines if the `INITIALIZE UPDATE` command is supported for any SD (without AM nor DM).	
ApduInstForExtraditionForSdWithAuthorizedManagement *Defines if the `INSTALL FOR EXTRADITION` command is supported for a SD with AM (also applies to the ISD).*	Y
ApduInstForInstallAndInstForMakeSelectableSupportForSdWithAuthorizedManagement *Defines if the `INSTALL FOR INSTALL AND MAKE SELECTABLE` command is supported for a SD with AM (also applies to the ISD).*	Y
ApduInstForLoadAndApduLoadSupportForSdWithAuthorizedManagement *Defines if the `INSTALL FOR LOAD` and `LOAD` commands are supported for a SD with AM (also applies to the ISD).*	Y
ApduInstForPersoSupportForSdWithAuthorizedManagement *Defines if the `INSTALL FOR PERSONALIZATION` command is supported for a SD with AM (also applies to the ISD).*	Y
ApduPutKeySupportForOtherSd *Defines if the `PUT KEY` command is supported for any SD (without AM nor DM).*	Y
ApduStoreDataSupportForOtherSd *Defines if the `STORE DATA` command is supported for any SD (without AM nor DM).*	Y
atLeastOneSupplementaryLc *Indicates that at least one supplementary logical channel is supported.*	Y
implementationSupportsSCP03 *Defines if SCP03 is supported by the UICC or not.*	O_MIFARE
implementationSupportsSCP81_TLS1_0 *Defines if TLS 1.0, as defined in RFC 2246 [14], is supported by the UICC or not.* see Note 1	O_TLS_10
implementationSupportsSCP81_TLS1_1 *Defines if TLS 1.1, as defined in RFC 4346 [15], is supported by the UICC or not.* see Note 1	O_TLS_11
implementationSupportsSCP81_TLS1_2 *Defines if TLS 1.2, as defined in RFC 5246 [16], is supported by the UICC or not.* see Note 1	O_TLS_12
scp81ImplementationSupportsAesDekKey *Defines if AES DEK key is supported by the UICC or not.*	O_AES_DEK
scp81ImplementationSupportsDesDekKey	Y

Test Suite Option	Support
Defines if DES DEK key is supported by the UICC or not.	
Note 1: The UUT shall support at least one of O_TLS_10, O_TLS_11 and O_TLS_12 options	

Table 20: UICC SCP81 Extension Test Suite - Options

3.1.8 Common Implementation Configuration Test Suite

The UUT may take the "Common_SCP03" package test cases of the "Common Implementation Configuration Test Suite Version 1.6.0" certification (depending of the O_MIFARE support). For the purpose of this document, this test suite shall only be used for testing the SCP03 support. Consequently, only the package "Common_SCP03" shall be executed by the Test Labs.

Note that if any revisions are performed on this test suite, the version 1.6.0.X, with X the number of the last revision, shall apply.

3.1.8.1 Technical Specifications

This certification relates to technical specifications listed in Table 21.

Technical Specifications
GlobalPlatform Card Technology - Secure Channel Protocol 03 - Card Specification v2.2 - Amendment D - Version 1.1

Table 21: Common Implementation Configuration Test Suite - SCP03 Technical Specification

3.1.8.2 Required Options Values

It shall be verified that in the `CardOptions.xml` file provided by the Manufacturer the "expected to be supported" options are set to true and the "expected not to be supported" options are set to false.

Note that in the table below, only the options that allow executing the SCP03 test cases are defined. See clause 3.1.1 for the format of Table 22.

Test Suite Option	Support
AmendmentCSupported *Defines if the "GlobalPlatform Card Amendment C [20]" is supported by the UICC or not. This is only relevant to determine if a life cycle state shall be encoded with 1 or 2 bytes.*	Y
ApduBeginRMACAndEndRMACSupported *Defines if the UICC supports `BEGIN RMAC` and `END RMAC` APDU commands.*	O_RMAC
ApduGetStatusSupportForOtherSd *Defines if the `GET STATUS` command is supported for any SD (without AM nor DM).*	Y
ApduInitializeUpdateSupportForOtherSD	Y

Test Suite Option	Support
Defines if the `INITIALIZE UPDATE` command is supported for any SD (without AM nor DM).	
ApduInstForInstallAndInstForMakeSelectableSupportForSdWithAuthorizedManagement *Defines if the `INSTALL FOR INSTALL AND MAKE SELECTABLE` command is supported for a SD with AM (also applies to the ISD).*	Y
ApduPutKeySupportForOtherSd *Defines if the `PUT KEY` command is supported for any SD (without AM nor DM).*	Y
atLeastOneSupplementaryLc *Indicates that at least one Supplementary Logical Channel is supported.*	Y
implementationSupportsSCP03 *Defines if SCP03 is supported by the UICC or not.*	Y
implementationSupportsSCP80 *Defines if SCP80 is supported by the UICC or not.*	Y
implementationSupportsTrustedPath *Defines if Trusted Path privilege is supported by the UICC or not.*	Y
implementationSupportSupplementarySD *Defines if SSD is supported by the UICC or not.*	Y
ISD_Configured_With_SCP03 *Defines if the ISD is configured with an SCP03 keyset.*	Y
ISD_Configured_With_SCP80 *Defines if the ISD is configured with an SCP80 keyset.*	Y
ISDHasCardResetPrivilege *Indicates if the ISD is required to have Card Reset privilege at the initial state.*	O_ISD_RST
ISDHasFinalApplicationPrivilege *Indicates if the ISD is required to have Final Application privilege at the initial state.*	O_ISD_FINAL

Table 22: Common Implementation Configuration Test Suite - SCP03 Options

3.2 Common Criteria

Certifications listed in this section are provided by the National Certification Body part of the CCRA.

3.2.1 (U)SIM Java Card Platform Protection Profile

The UUT should take the “EAL4+ Common Criteria” certification for the specification present in Table **23**.

Specification
(U)SIM Java Card Platform Protection Profile specification

Table 23: (U)SIM Java Card Platform Protection Profile - Specification

4 Test Specifications

Some test specifications have been developed by external organisations (EMVCo, ISO, ETSI). These organisations defined their own requirements for test benches, test applicability and pass criteria.

This section lists the test specifications that relate to the GSMA requirements [1].

4.1 Format of the Table of Test Specification Options

To execute the test cases related to some test specifications, the Manufacturer shall state support of different options. For some test specifications described in the following sections, a table, containing the expected options values, is specified.

The columns of this table have the following meaning:

Column	Meaning
Test Specification Option	The “Test Specification Option” column contains the name (if exists) and the description of the option defined by the related external organisation.
Support	The support columns are to be filled in by the Manufacturer. The following common notations are used for the support column: Y or y: expected to be supported by the implementation. N or n: expected to not be supported by the implementation. O_XYZ: refers to the support of the related feature described in Table 4.

Table 24: Format of the Table of Test Specification Options

4.2 ETSI TS 102 268

The UUT shall take test cases defined in the “ETSI TS 102 268” test specification [4] in order to check its compliance with “ETSI TS 102 241” technical specification [8].

All the mandatory test cases are applicable according to the applicability of the referred ETSI test specification.

4.3 ETSI TS 103 115

The UUT shall take test cases defined in the “ETSI TS 103 115” test specification [5] in order to check its compliance with “ETSI TS 102 705” technical specification [9].

All the test cases shall be applicable according to Table 4.2 a) of the ETSI test specification [5] except the test defined in clause 6.1.2.5 (method requestCallbackNotification) that shall not be performed.

The table below defines the options which shall be used to execute the different test cases. See clause 4.1 for the format of Table 25.

Test Specification Option	Support
O_CE_TYPE_A *Defines if card emulation, Type A is supported on the UICC or not.*	Y
O_CE_TYPE_B *Defines if card emulation, Type B is supported by the UICC or not.*	Y
O_CE_TYPE_B_PRIME *Defines if card emulation, Type B' is supported by the UICC or not.*	O_CE_TBP
O_CE_TYPE_F *Defines if card emulation, Type F is supported by the UICC or not.*	O_CE_TF
O_MSG_GT_BUF *Indicates if the HCP message size greater than supported buffer size.*	O_HCP
O_RM_TYPE_A *Defines if reader mode, Type A is supported by the UICC or not.*	O_RM_TA
O_RM_TYPE_B *Defines if reader mode, Type B is supported by the UICC or not.*	O_RM_TB

Table 25: ETSI TS 103 115 Test Specification - Options

4.4 ETSI TS 102 431

The UUT may take test cases defined in the "ETSI TS 102 431" [10] in order to check its compliance with "ETSI TS 102 127" technical specification [11] (depending of the O_CATTP support).

All the test cases shall be applicable according to the applicability table presented in section 5.1 of the ETSI test specification [10].

The table below defines the options which shall be used to execute the different test cases. See clause 4.1 for the format of Table 26.

Test Specification Option	Support
Defines if window size > 1 is supported by the UICC or not.	O_WIN_S
Defines if simultaneous open requests are supported by the UICC or not.	O_SOPEN
Defines if segmentation of outgoing data is supported by the UICC or not.	O_SEG
Defines if local port definition in active open request is supported by the UICC or not.	O_LPORT
Defines if simultaneous open requests and local port definition in active open request are supported by the UICC or not.	O_SOPEN AND O_LPORT
Defines if active mode is supported by the UICC or not.	Y
Defines if passive mode is supported by the UICC or not.	O_PASS_M

Table 26: ETSI TS 102 431 Test Specification - Options

4.5 ETSI TS 102 226 Testing

The test cases that allow the compliance of the UICC with the “ETSI TS 102 226” technical specification [17] to be checked are defined as FFS.

5 Other Tests Cases

Test cases described in this section are complementary to the test cases required to obtain certifications listed in section 3 and the test cases defined in test specifications listed in section 4.

5.1 Cryptographic Algorithms

5.1.1 General Overview

This section defines some test cases related to cryptographic algorithms that shall be supported by the UICC.

5.1.2 Conformance Requirements

All the following GSMA UICC requirements refer to the ETSI TS 102 225 [18].

Ref	Section	REQ	Description
[1]	3.1.9	RQ1	The UICC shall support AES cryptographic algorithm with 128 bits key length.
[1]	3.1.9	RQ2	The UICC shall support AES cryptographic algorithm with 256 bits key length.
[1]	3.1.9	RQ3	The UICC shall support 3DES cryptographic algorithm with 24 bytes key length.

5.1.3 Constants Definition

Listed are the different constants that shall be used to execute the test cases defined in section 5.1.5. A constant present in the table below is referenced in the test sequences as follow: `#CONSTANT_NAME` (e.g. `#AES_KEY_ID1_16` refers to the value of the constant named “AES_KEY_ID1_16”).

Constant Name	Value in Hexadecimal String
AES_KEY_ID1_16	11 22 33 44 55 66 77 88 AA 22 33 44 55 66 77 88
AES_KEY_ID1_32	11 22 33 44 55 66 77 88 AA 22 33 44 55 66 77 88 BB 22 33 44 55 66 77 88 CC 22 33 44 55 66 77 88
AES_KEY_ID2_16	11 22 33 44 55 66 77 88 BB 22 33 44 55 66 77 88
AES_KEY_ID2_32	11 22 33 44 55 66 77 88 DD 22 33 44 55 66 77 88 EE 22 33 44 55 66 77 88 FF 22 33 44 55 66 77 88
AES_KEY_ID3_16	11 22 33 44 55 66 77 88 CC 22 33 44 55 66 77 88
AES_KEY_ID3_32	11 22 33 44 55 66 77 88 00 22 33 44 55 66 77 88 11 22 33 44 55 66 77 88 22 22 33 44 55 66 77 88
ELF_SD_AID	A0 00 00 01 51 53 50
EM_SD_AID	A0 00 00 01 51 53 50 41
ISD_AID	A0 00 00 01 51 00 00 00
SCP80_COUNTER	00 00 00 00 01
SCP80_SD_AID	A0 00 00 05 59 10 10 01 11 22 33 01
SD_TAR	11 22 33

5.1.4 Referenced APDUs

Listed are the different APDUs that shall be used to execute the test cases defined in section 5.1.5. An APDU present in the table below is referenced in the test sequences as follow: `[APDU_NAME]` (e.g. `[SELECT_ISD]` refers to the value of the APDU named "SELECT_ISD").

APDU Name	Value in Hexadecimal String
INSTALL_SCP80_SD	- CLA = 80 - INS = E6 - P1 = 0C - P2 = 00 - LC = 39 - Data = 07 #ELF_SD_AID 08 #EM_SD_AID 0C #SCP80_SD_AID 03 80 80 00 15 EA 0D 80 0B 01 00 00 00 00 00 03 #SD_TAR 00 C9 04 81 02 80 00 00 - LE = 00
GET_DATA_E0	- CLA = 80 - INS = CA - P1 = 00 - P2 = E0 - LE = 00
GET_STATUS_SD	- CLA = 80 - INS = F2 - P1 = 40 - P2 = 02 - LC = 13 - Data = 4F 0C #SCP80_SD_AID 5C 03 4F 9F 70 - LE = 00
PUT_SCP_AES_KEYS_16	- CLA = 80 - INS = D8 - P1 = 00 - P2 = 81 - LC = 47 - Data = 01 88 11 10 ENC_KENC_16 03 KCV1 88 12 10 ENC_KMAC_16 08 03 KCV2 88 11 10 ENC_DEK_16 03 KCV3 - LE = 00 see Note 1 and Note 3
PUT_SCP_AES_KEYS_32	- CLA = 80 - INS = D8 - P1 = 00 - P2 = 81 - LC = 77 - Data = 01 88 21 20 ENC_KENC_32 03 KCV1 88 22 20 ENC_KMAC_32 08 03 KCV2 88 21 20 ENC_DEK_32 03 KCV3 - LE = 00 see Note 2 and Note 3
SELECT_ISD	- CLA = 00 - INS = A4

	- P1 = 04 - P2 = 00 - LC = 08 - Data = #ISD_AID
SELECT_SCP80_SD	- CLA = 00 - INS = A4 - P1 = 04 - P2 = 00 - LC = 0C - Data = #SCP80_SD_AID
TERMINAL_PROFILE	- CLA = 80 - INS = 10 - P1 = 00 - P2 = 00 - LC = 14 - Data = FF FF FF FF 7F 0D 00 DF FF 00 00 1F A2 01 0A 86 1F 40 00 00
Note 1: The ENC_KENC_16, ENC_KMAC_16 and ENC_DEK_16 refer respectively to the #AES_KEY_ID1_16, #AES_KEY_ID2_16 and #AES_KEY_ID3_16 encrypted with the DEK of the current SCP session. *Note 2: The ENC_KENC_32, ENC_KMAC_32 and ENC_DEK_32 refer respectively to the #AES_KEY_ID1_32, #AES_KEY_ID2_32 and #AES_KEY_ID3_32 encrypted with the DEK of the current SCP session.* *Note 3: KCV1, KCV2 and KCV3 refer to the key check values computed by encrypting 16 bytes, each with value '01', with the related SCP key, retaining the 3 highest-order bytes of the encrypted result.*	

5.1.5 Test Cases

This section defines the test cases that allow testing of the requirements listed in section 5.1.2.

5.1.5.1 TC.AES.16.SCP80: SCP80 using AES with 16 bytes key length

Test Purpose

To ensure that SCP80 is supported using AES with 16 bytes key length. After creating and personalizing an SD, an SMS envelope containing a GET STATUS command is sent using AES security. Note that different SCP80 security levels are used in the test sequences defined below. In terms of KID, only CC, considered as the most common algorithm, is tested.

Referenced Requirement

- RQ1

Initial Conditions

- No Application identified by the AID `#SCP80_SD_AID` is present on the UUT
- SCP02 keyset initialized on ISD
  - The corresponding Triple DES keys values are named, in the test sequences below, `SCP02_ISD_KENC`, `SCP02_ISD_KMAC` and `SCP02_ISD_DEK`
- SCP80 AES keyset initialized on ISD
  - The corresponding keys length shall be 16 bytes
  - The length of the MAC related to the CC is defined with 8 bytes
  - The AES keys values are named, in the test sequences below, `SCP80_ISD_KENC`, `SCP80_ISD_KMAC` and `SCP80_ISD_DEK`

5.1.5.1.1 Test Sequence N°1: With SPI=’1221’

Initial Conditions

- None

Step	Direction	Sequence / Description	Expected Result
1	DS → UUT	RESET	ATR returned by UUT
2	DS → UUT	[SELECT_ISD]	
3	UUT → DS	ATS	SW='9000'
4	DS → UUT	Open an SCP02 session using INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands as defined in GlobalPlatform Card Specification [13]. The SCP02_ISD_KENC, SCP02_ISD_KMAC and SCP02_ISD_DEK shall be used. The security level used shall be AUTHENTICATED and C-MAC. see Note 1	
5	UUT → DS	Answer a SW for each command	SW='9000' for both commands
6	DS → UUT	[INSTALL_SCP80_SD] secured with the SCP02 session keys	
7	UUT → DS	Answer a SW	SW='9000'
8	DS → UUT	RESET	ATR returned by UUT
9	DS → UUT	[TERMINAL_PROFILE]	Toolkit initialization (see Note 2) SW='9000'
10	DS → UUT	ENVELOPE (SMS-PP DOWNLOAD) containing a secured packet as defined in ETSI TS 102 225 [18]. The APDU to send is [PUT_SCP_AES_KEYS_16]. The SCP80_ISD_KMAC shall be used to generate the CC. The SCP80_ISD_DEK shall be used to cipher the keys within the PUT KEY command. The CC shall be 8 bytes long. The TAR #SD_TAR shall be used. The counter shall be adapted according its current value on the ISD keyset. The SPI '1221' shall be used. The KIC '00' shall be used. The KID 'X2' shall be used ('X' is equal to the KVN of the ISD keyset). Expanded data format with definite length, as defined in ETSI TS 102 226 [17], shall be used.	

Step	Direction	Sequence / Description	Expected Result
11	UUT → DS	*PROACTIVE COMMAND PENDING:* SEND SHORT MESSAGE	
12	DS → UUT	FETCH	
13	UUT → DS	*PROACTIVE COMMAND:* SEND SHORT MESSAGE	1. The response packet contains additional response data in expanded format with definite length 2. R-APDU contains a. The KVN ‘01’ followed by the three KCV used in the `PUT KEY` command (i.e. `[PUT_SCP_AES_KEYS_16]`) b. SW=’9000’
14	DS → UUT	TERMINAL RESPONSE	SW=’9000’
15	DS → UUT	ENVELOPE (SMS-PP DOWNLOAD) containing a secured packet as defined in ETSI TS 102 225 [18]. The APDU to send is `[GET_STATUS_SD]`. The `#AES_KEY_ID2_16` shall be used to generate the CC. The CC shall be 8 bytes long. The TAR `#SD_TAR` shall be used. The counter shall be set to `#SCP80_COUNTER`. The SPI ‘1221’ shall be used. The KIC ‘00’ shall be used. The KID ‘12’ shall be used. Expanded data format with definite length, as defined in ETSI TS 102 226 [17], shall be used.	
16	UUT → DS	*PROACTIVE COMMAND PENDING:* SEND SHORT MESSAGE	
17	DS → UUT	FETCH	
18	UUT → DS	*PROACTIVE COMMAND:* SEND SHORT MESSAGE	1. The response packet contains additional response data in expanded format with definite length 2. R-APDU contains the tag ‘E3’ a. The lifecycle state (i.e. ‘9F70’) of the SD is personalized (i.e. ‘0F’) b. SW=’9000’

Step	Direction	Sequence / Description	Expected Result
19	DS → UUT	TERMINAL RESPONSE	SW=’9000’
20	DS → UUT	[SELECT_SCP80_SD]	
21	UUT → DS	ATS	SW=’9000’
22	DS → UUT	[GET_DATA_E0]	
23	UUT → DS	Answer an R-APDU	1. SW=’9000’ 2. Tag ‘E0’ is returned 3. Three Key Information Data (i.e. ‘C0’) are part of the tag ‘E0’ a. Each key type is AES (i.e. ‘88’) b. Each key length is equal to 16
Note 1: To avoid conflict with the support of several SCPs (e.g. both SCP02 and SCP03), the SCP02 session shall be open on an explicit KVN (i.e. the one created during the UICC manufacturing). *Note 2: It is assumed that some proactive commands may be sent by the UICC after sending the TERMINAL PROFILE (i.e. SET UP EVENT LIST, POLL INTERVAL, PROVIDE LOCAL INFORMATION…). In this case, the DS shall send the corresponding FETCH and TERMINAL RESPONSE (successfully performed) commands.*			

5.1.5.1.2 Test Sequence N°2: With SPI=’1639’

Initial Conditions

- None

Step	Direction	Sequence / Description	Expected Result
1	DS → UUT	RESET	ATR returned by UUT
2	DS → UUT	[SELECT_ISD]	
3	UUT → DS	ATS	SW=’9000’
4	DS → UUT	Open an SCP02 session using INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands as defined in GlobalPlatform Card Specification [13]. The SCP02_ISD_KENC, SCP02_ISD_KMAC and SCP02_ISD_DEK shall be used. The security level used shall be AUTHENTICATED and C-MAC. see Note 1	
5	UUT → DS	Answer a SW for each command	SW=’9000’ for both commands
6	DS → UUT	[INSTALL_SCP80_SD] secured with the SCP02 session keys	

Step	Direction	Sequence / Description	Expected Result
7	UUT → DS	Answer a SW	SW=’9000’
8	DS → UUT	RESET	ATR returned by UUT
9	DS → UUT	[TERMINAL_PROFILE]	Toolkit initialization (see Note 2) SW=’9000’
10	DS → UUT	ENVELOPE (SMS-PP DOWNLOAD) containing a secured packet as defined in ETSI TS 102 225 [18]. The APDU to send is [PUT_SCP_AES_KEYS_16]. The SCP80_ISD_KENC shall be used to cipher the secured packet. The SCP80_ISD_KMAC shall be used to generate the CC. The SCP80_ISD_DEK shall be used to cipher the keys within the PUT KEY command. The CC shall be 8 bytes long. The TAR #SD_TAR shall be used. The counter shall be adapted according its current value on the ISD keyset. The SPI ‘1639’ shall be used. The KIC ‘X2’ shall be used (‘X’ is equal to the KVN of the ISD keyset). The KID ‘X2’ shall be used (‘X’ is equal to the KVN of the ISD keyset). Expanded data format with definite length, as defined in ETSI TS 102 226 [17], shall be used.	
11	UUT → DS	*PROACTIVE COMMAND PENDING:* SEND SHORT MESSAGE	
12	DS → UUT	FETCH	

Step	Direction	Sequence / Description	Expected Result
13	UUT → DS	*PROACTIVE COMMAND:* SEND SHORT MESSAGE	1. The response packet is ciphered with the SCP80_ISD_KENC 2. The response packet contains a CC (8 bytes long) generated with the SCP80_ISD_KMAC 3. The response packet contains additional response data in expanded format with definite length 4. R-APDU contains a. The KVN '01' followed by the three KCV used in the PUT KEY command (i.e. [PUT_SCP_AES_KEYS_16]) b. SW='9000'
14	DS → UUT	TERMINAL RESPONSE	SW='9000'
15	DS → UUT	ENVELOPE (SMS-PP DOWNLOAD) containing a secured packet as defined in ETSI TS 102 225 [18]. The APDU to send is [GET_STATUS_SD]. The #AES_KEY_ID1_16 shall be used to cipher the secured packet. The #AES_KEY_ID2_16 shall be used to generate the CC. The CC shall be 8 bytes long. The TAR #SD_TAR shall be used. The counter shall be set to #SCP80_COUNTER. The SPI '1639' shall be used. The KIC '12' shall be used. The KID '12' shall be used. Expanded data format with definite length, as defined in ETSI TS 102 226 [17], shall be used.	
16	UUT → DS	*PROACTIVE COMMAND PENDING:* SEND SHORT MESSAGE	
17	DS → UUT	FETCH	

Step	Direction	Sequence / Description	Expected Result
18	UUT → DS	*PROACTIVE COMMAND:* SEND SHORT MESSAGE	1. The response packet is ciphered with the `#AES_KEY_ID1_16` 2. The response packet contains a CC (8 bytes long) generated with the `#AES_KEY_ID2_16` 3. The response packet contains additional response data in expanded format with definite length 4. R-APDU contains the tag ‘E3’ a. The lifecycle state (i.e. ‘9F70’) of the SD is personalized (i.e. ‘0F’) b. SW=’9000’
19	DS → UUT	TERMINAL RESPONSE	SW=’9000’
20	DS → UUT	`[SELECT_SCP80_SD]`	
21	UUT → DS	ATS	SW=’9000’
22	DS → UUT	`[GET_DATA_E0]`	
23	UUT → DS	Answer an R-APDU	1. SW=’9000’ 2. Tag ‘E0’ is returned 3. Three Key Information Data (i.e. ‘C0’) are part of the tag ‘E0’ a. Each key type is AES (i.e. ‘88’) b. Each key length is equal to 16
Note 1: To avoid conflict with the support of several SCPs (e.g. both SCP02 and SCP03), the SCP02 session shall be open on an explicit KVN (i.e. the one created during the UICC manufacturing). *Note 2: It is assumed that some proactive commands may be sent by the UICC after sending the TERMINAL PROFILE (i.e. SET UP EVENT LIST, POLL INTERVAL, PROVIDE LOCAL INFORMATION…). In this case, the DS shall send the corresponding FETCH and TERMINAL RESPONSE (successfully performed) commands.*			

5.1.5.2 TC.AES.32.SCP80: SCP80 using AES with 32 bytes key length

Test Purpose

To ensure that SCP80 is supported using AES with 32 bytes key length. After creating and personalizing an SD, an SMS envelope containing a GET STATUS command is sent using AES security. Note that different SCP80 security levels are used in the test sequences defined below. In terms of KID, only CC, considered as the most common algorithm, is tested.

Referenced Requirement

- RQ2

Initial Conditions

- No Application identified by the AID `#SCP80_SD_AID` is present on the UUT
- SCP02 keyset initialized on ISD
  - The corresponding Triple DES keys values are named, in the test sequences below, `SCP02_ISD_KENC`, `SCP02_ISD_KMAC` and `SCP02_ISD_DEK`
- SCP80 AES keyset initialized on ISD
  - The corresponding keys length shall be 32 bytes
  - The length of the MAC related to the CC is defined with 8 bytes
  - The AES keys values are named, in the test sequences below, `SCP80_ISD_KENC`, `SCP80_ISD_KMAC` and `SCP80_ISD_DEK`

5.1.5.2.1 Test Sequence N°1: With SPI='1221'

Initial Conditions

- None

Step	Direction	Sequence / Description	Expected Result
1	DS → UUT	RESET	ATR returned by UUT
2	DS → UUT	`[SELECT_ISD]`	
3	UUT → DS	ATS	SW='9000'
4	DS → UUT	Open an SCP02 session using `INITIALIZE UPDATE` and `EXTERNAL AUTHENTICATE` commands as defined in GlobalPlatform Card Specification [13]. The `SCP02_ISD_KENC`, `SCP02_ISD_KMAC` and `SCP02_ISD_DEK` shall be used. The security level used shall be `AUTHENTICATED` and `C-MAC`. see Note 1	
5	UUT → DS	Answer a SW for each command	SW='9000' for both commands
6	DS → UUT	`[INSTALL_SCP80_SD]` secured with the SCP02 session keys	
7	UUT → DS	Answer a SW	SW='9000'
8	DS → UUT	RESET	ATR returned by UUT
9	DS → UUT	`[TERMINAL_PROFILE]`	Toolkit initialization (see Note 2) SW='9000'

Step	Direction	Sequence / Description	Expected Result
10	DS → UUT	ENVELOPE (SMS-PP DOWNLOAD) containing a secured packet as defined in ETSI TS 102 225 [18]. The APDU to send is `[PUT_SCP_AES_KEYS_32]`. The `SCP80_ISD_KMAC` shall be used to generate the CC. The `SCP80_ISD_DEK` shall be used to cipher the keys within the `PUT KEY` command. The CC shall be 8 bytes long. The TAR `#SD_TAR` shall be used. The counter shall be adapted according its current value on the ISD keyset. The SPI '1221' shall be used. The KIC '00' shall be used. The KID 'X2' shall be used ('X' is equal to the KVN of the ISD keyset). Expanded data format with definite length, as defined in ETSI TS 102 226 [17], shall be used.	
11	UUT → DS	*PROACTIVE COMMAND PENDING:* SEND SHORT MESSAGE	
12	DS → UUT	FETCH	
13	UUT → DS	*PROACTIVE COMMAND:* SEND SHORT MESSAGE	1. The response packet contains additional response data in expanded format with definite length 2. R-APDU contains a. The KVN '01' followed by the three KCV used in the `PUT KEY` command (i.e. `[PUT_SCP_AES_KEYS_32]`) b. SW='9000'
14	DS → UUT	TERMINAL RESPONSE	SW='9000'

Step	Direction	Sequence / Description	Expected Result
15	DS → UUT	ENVELOPE (SMS-PP DOWNLOAD) containing a secured packet as defined in ETSI TS 102 225 [18]. The APDU to send is `[GET_STATUS_SD]`. The `#AES_KEY_ID2_32` shall be used to generate the CC. The CC shall be 8 bytes long. The TAR `#SD_TAR` shall be used. The counter shall be set to `#SCP80_COUNTER`. The SPI '1221' shall be used. The KIC '00' shall be used. The KID '12' shall be used. Expanded data format with definite length, as defined in ETSI TS 102 226 [17], shall be used.	
16	UUT → DS	*PROACTIVE COMMAND PENDING:* SEND SHORT MESSAGE	
17	DS → UUT	FETCH	
18	UUT → DS	*PROACTIVE COMMAND:* SEND SHORT MESSAGE	1. The response packet contains additional response data in expanded format with definite length 2. R-APDU contains the tag 'E3' a. The lifecycle state (i.e. '9F70') of the SD is personalized (i.e. '0F') b. SW='9000'
19	DS → UUT	TERMINAL RESPONSE	SW='9000'
20	DS → UUT	`[SELECT_SCP80_SD]`	
21	UUT → DS	ATS	SW='9000'
22	DS → UUT	`[GET_DATA_E0]`	
23	UUT → DS	Answer an R-APDU	1. SW='9000' 2. Tag 'E0' is returned 3. Three Key Information Data (i.e. 'C0') are part of the tag 'E0' a. Each key type is AES (i.e. '88') b. Each key length is equal to 32

Step	Direction	Sequence / Description	Expected Result
Note 1: To avoid conflict with the support of several SCPs (e.g. both SCP02 and SCP03), the SCP02 session shall be open on an explicit KVN (i.e. the one created during the UICC manufacturing). *Note 2: It is assumed that some proactive commands may be sent by the UICC after sending the TERMINAL PROFILE (i.e. SET UP EVENT LIST, POLL INTERVAL, PROVIDE LOCAL INFORMATION…). In this case, the DS shall send the corresponding FETCH and TERMINAL RESPONSE (successfully performed) commands.*			

5.1.5.2.2 Test Sequence N°2: With SPI='1639'

Initial Conditions

- None

Step	Direction	Sequence / Description	Expected Result
1	DS → UUT	RESET	ATR returned by UUT
2	DS → UUT	[SELECT_ISD]	
3	UUT → DS	ATS	SW='9000'
4	DS → UUT	Open an SCP02 session using INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands as defined in GlobalPlatform Card Specification [13]. The SCP02_ISD_KENC, SCP02_ISD_KMAC and SCP02_ISD_DEK shall be used. The security level used shall be AUTHENTICATED and C-MAC. see Note 1	
5	UUT → DS	Answer a SW for each command	SW='9000' for both commands
6	DS → UUT	[INSTALL_SCP80_SD] secured with the SCP02 session keys	
7	UUT → DS	Answer a SW	SW='9000'
8	DS → UUT	RESET	ATR returned by UUT
9	DS → UUT	[TERMINAL_PROFILE]	Toolkit initialization (see Note 2) SW='9000'

Step	Direction	Sequence / Description	Expected Result
10	DS → UUT	ENVELOPE (SMS-PP DOWNLOAD) containing a secured packet as defined in ETSI TS 102 225 [18]. The APDU to send is `[PUT_SCP_AES_KEYS_32]`. The `SCP80_ISD_KENC` shall be used to cipher the secured packet. The `SCP80_ISD_KMAC` shall be used to generate the CC. The `SCP80_ISD_DEK` shall be used to cipher the keys within the `PUT KEY` command. The CC shall be 8 bytes long. The TAR `#SD_TAR` shall be used. The counter shall be adapted according its current value on the ISD keyset. The SPI '1639' shall be used. The KIC 'X2' shall be used ('X' is equal to the KVN of the ISD keyset). The KID 'X2' shall be used ('X' is equal to the KVN of the ISD keyset). Expanded data format with definite length, as defined in ETSI TS 102 226 [17], shall be used.	
11	UUT → DS	*PROACTIVE COMMAND PENDING:* SEND SHORT MESSAGE	
12	DS → UUT	FETCH	
13	UUT → DS	*PROACTIVE COMMAND:* SEND SHORT MESSAGE	1. The response packet is ciphered with the `SCP80_ISD_KENC` 2. The response packet contains a CC (8 bytes long) generated with the `SCP80_ISD_KMAC` 3. The response packet contains additional response data in expanded format with definite length 4. R-APDU contains a. The KVN '01' followed by the three KCV used in the `PUT KEY` command (i.e. `[PUT_SCP_AES_KEYS_32]`) b. SW='9000'
14	DS → UUT	TERMINAL RESPONSE	SW='9000'

Step	Direction	Sequence / Description	Expected Result
15	DS → UUT	ENVELOPE (SMS-PP DOWNLOAD) containing a secured packet as defined in ETSI TS 102 225 [18]. The APDU to send is `[GET_STATUS_SD]`. The `#AES_KEY_ID1_32` shall be used to cipher the secured packet. The `#AES_KEY_ID2_32` shall be used to generate the CC. The CC shall be 8 bytes long. The TAR `#SD_TAR` shall be used. The counter shall be set to `#SCP80_COUNTER`. The SPI '1639' shall be used. The KIC '12' shall be used. The KID '12' shall be used. Expanded data format with definite length, as defined in ETSI TS 102 226 [17], shall be used.	
16	UUT → DS	*PROACTIVE COMMAND PENDING:* SEND SHORT MESSAGE	
17	DS → UUT	FETCH	
18	UUT → DS	*PROACTIVE COMMAND:* SEND SHORT MESSAGE	1. The response packet is ciphered with the `#AES_KEY_ID1_32` 2. The response packet contains a CC (8 bytes long) generated with the `#AES_KEY_ID2_32` 3. The response packet contains additional response data in expanded format with definite length 4. R-APDU contains the tag 'E3' a. The lifecycle state (i.e. '9F70') of the SD is personalized (i.e. '0F') b. SW='9000'
19	DS → UUT	TERMINAL RESPONSE	SW='9000'
20	DS → UUT	`[SELECT_SCP80_SD]`	
21	UUT → DS	ATS	SW='9000'
22	DS → UUT	`[GET_DATA_E0]`	

Step	Direction	Sequence / Description	Expected Result
23	UUT → DS	Answer an R-APDU	1. SW='9000' 2. Tag 'E0' is returned 3. Three Key Information Data (i.e. 'C0') are part of the tag 'E0' a. Each key type is AES (i.e. '88') b. Each key length is equal to 32
Note 1: To avoid conflict with the support of several SCPs (e.g. both SCP02 and SCP03), the SCP02 session shall be open on an explicit KVN (i.e. the one created during the UICC manufacturing). *Note 2: It is assumed that some proactive commands may be sent by the UICC after sending the TERMINAL PROFILE (i.e. SET UP EVENT LIST, POLL INTERVAL, PROVIDE LOCAL INFORMATION…). In this case, the DS shall send the corresponding FETCH and TERMINAL RESPONSE (successfully performed) commands.*			

5.1.5.3 TC.3DES.24.SCP80: SCP80 using Triple DES with 24 bytes key length

Development of the test cases related to the support of SCP80 using Triple DES with 24 bytes key length is defined as FFS.

5.2 ACTIVATE Proactive Command

5.2.1 General Overview

This section verifies the support of proactive command ACTIVATE by the UICC.

5.2.2 Conformance Requirements

The following GSMA UICC requirement refers to the ETSI TS 102 223 [22].

Ref	Section	REQ	Description
[1]	3	RQ4	The UICC shall support proactive command ACTIVATE.

5.2.3 Test Cases

Development of the test cases related to this proactive command is defined as FFS.

5.3 CASD Management Data

5.3.1 General Overview

This section defines some test cases related to the CASD management data.

5.3.2 Conformance Requirements

Ref	Section	REQ	Description
[19]	9.1	RQ5	For interoperability purposes, the CASD is required to expose its capabilities so that off-card entities know which confidential SD personalization scenarios are supported by the card.

5.3.3 Test Cases

Development of the test cases related to the CASD management data is defined as FFS.

Annex A SP Applications

This section presents recommended complementary rules to be taken into account for developing Java Card applets.

In this document the Basic Application and Sensitive Application terms refer to the definitions of the GlobalPlatform specification [3].

A.1 Basic Application

A Basic Application is an Application that is not required to be certified. The Test Book refers to applet development guidelines [2] to provide to SP some rules, in order to properly develop their NFC service applet.

All Basic Applications that are pre-loaded or dynamically loaded in a NFC UICC should be compliant with this guideline.

A.2 Sensitive Application

A Sensitive Application is an Application that requires security certification by an evaluation scheme such as Common Criteria. All these Applications (bank, transport...) that are used in a NFC UICC should be certified according their own evaluation scheme.

Annex B Java Card

The UICC shall support Java Card™ Platform, Version 3.0.1 Classic Edition. The Integer data type shall be mandatory for the Java Card Virtual Machine. Java Card Technology Compatibility Kit (TCK) shall be used to test these requirements. The UICC manufacturer shall be able to provide the Java Card TCK report to the MNOs.

Annex C Document Management

C.1 Document History

Version	Date	Brief description of change	Editor / Company
1.0	25/02/2015	First release	Sébastien Kuras, FIME

C.2 Document Owner

Type	Description
Document Owner	GSMA SIM Group
Editor / Company	Sébastien Kuras, FIME

Other Information

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com.

Your comments or suggestions & questions are always welcome.